INL/JOU-18-45648-Revision-0

Modeling and Analysis of Eavesdropping Attack in 802.11ad mmWave Wireless Networks

Arup Bhuyan, Zhi Sun, Sarankumar Balakrishnan, Pu Wang

May 2019

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/JOU-18-45648-Revision-0

Modeling and Analysis of Eavesdropping Attack in 802.11ad mmWave Wireless Networks

Arup Bhuyan, Zhi Sun, Sarankumar Balakrishnan, Pu Wang

May 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 4, 2019, accepted May 6, 2019, date of publication May 28, 2019, date of current version June 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2919674

Modeling and Analysis of Eavesdropping Attack in 802.11ad mmWave Wireless Networks

SARANKUMAR BALAKRISHNAN[1], (Student Member, IEEE), PU WANG[2], (Member, IEEE), ARUPJYOTI BHUYAN[3], (Senior Member, IEEE), AND ZHI SUN[1], (Member, IEEE)

[1]Department of Electrical Engineering, University at Buffalo, The State University of New York, Buffalo, NY 14260, USA
[2]Department of Computer Science, University of North Carolina at Charlotte, Charlotte, NC 28223, USA
[3]Idaho National Laboratory, Idaho Falls, ID 83402, USA

Corresponding author: Sarankumar Balakrishnan (sarankum@buffalo.edu)

This work was supported by the INL Laboratory Directed Research and Development (LDRD) Program under DOE Idaho Operations Office under Grant DE-AC07-05ID14517.

ABSTRACT Next generation wireless communication networks utilizing 60 GHz millimeter wave (mmWave) frequency bands are expected to achieve multi-gigabit throughput with the use of highly directional phased-array antennas. These directional signal beams provide enhanced security to the legitimate networks due to the increased difficulties of eavesdropping. However, there still exists significant possibility of eavesdropping since 1) the reflections of the signal beam from ambient reflectors enables opportunistic stationary eavesdropping attacks, and; 2) carefully designed beam exploration strategy enables active nomadic eavesdropping attack. This paper discusses eavesdropper attack strategies for 802.11ad mmWave systems and provides the first analytical model to characterize the success possibility of eavesdropping in both opportunistic stationary attacks and active nomadic attacks. We derive the success probability of eavesdropping considering the ambient reflectors in the environment and errors introduced in the beam exploration strategies of the proposed eavesdropping attacker models. We study the success probability for both opportunistic stationary attack scenario and active nomadic attack scenario through numerical simulations. In addition to numerical simulations, we also evaluate the proposed attacker models using an 802.11ad test bed consisting of commercially available off-the-shelf devices.

INDEX TERMS Millimeter wave communications, 802.11ad, stochastic geometry, success probability, eavesdropping attack.

I. INTRODUCTION

Millimeter wave (mmWave) communication is considered to be one of the key enabling technologies of next generation very high throughput wireless networks. MmWave frequency bands have different propagation characteristics than those at lower microwave frequencies. At mmWave frequencies, the signal experiences high attenuation due to propagation and penetration losses [1]. When compared to microwave frequencies at sub 6 GHz band, 60 GHz mmWave frequency bands experience additional 20 dB signal attenuation. The IEEE 802.11ad standard [2] addresses these challenges by using high gain directional antennas to overcome the signal attenuation at 60 GHz. IEEE 802.11ad leverages the wide bandwidth available at 60 GHz frequency band and data-rates of around 7 Gbps are envisioned with the use of beamforming with phased-array antennas to steer around the obstacles.

With the expected proliferation of 802.11ad based mmWave WLAN for high throughput indoor connectivity, security of these wireless networks becomes a critical issue. Contrary to the omni-directional signal transmission in legacy 802.11 based wireless networks operating at 2.4 and 5 GHz microwave band, 60 GHz 802.11ad mmWave networks are characterized by highly directional transmission enabled by beamforming [1]. 802.11ad standard specifies a minimum beamwidth of 3 degrees. Conventionally it is believed that the very narrow beamwidth offers inherent PHY security against eavesdroppers. However, such optimistic conclusion is based on the assumption that eavesdroppers only rely on the line of sight (LOS) link to the legitimate devices and do not have any information of the direction of the beam used by the legitimate devices.

The associate editor coordinating the review of this manuscript and approving it for publication was Waleed Ejaz.

In practice, there still exists significant possibility of eavesdropping in 802.11ad mmWave systems. On the one hand, many millimeter wave indoor experimental measurements have shown that first order reflections from structures in an indoor environment contributes to majority of signal power in non-line-of-sight (NLOS) [3]. Thus, in 60 GHz mmWave communication, along with LOS, first order reflections from ambient reflectors play a crucial role in the signal coverage of such systems. As a result, even when not in the LOS region of the narrow mmWave beam, it is still possible for the eavesdropper to overhear the transmission due to the multiple reflection paths. On the other hand, to establish the highly directional mmWave link, the legitimate transmitter and receiver need to scan all the possible direction sectors to search the optimal beam between themselves [2]. Due to this beam searching procedure [4], eavesdropper can estimate the LOS region of the beam selected by the legitimate users. Once the eavesdropper moves to the LOS region, the possibility of successful eavesdropping will dramatically increase.

To date, the understanding of the eavesdropping attack in 802.11ad mmWave WLAN system is still limited to experimental results. In [5], a multi-antenna eavesdropping attack strategy is proposed. The ability of the eavesdropper to reliably detect the intentional jamming from the legitimate transmitter is experimentally demonstrated. In [6], an attack on the antenna subset modulation (ASM) technique is developed based on compressive sensing technique. In [7], the impact of reflections on the physical layer security of mmWave systems are experimentally demonstrated. It shows that the eavesdropper can successfully eavesdrop even highly directional signal beams when small-scale reflectors are placed along the direction of the main beam. The work in [8] presents experimental study on the side-lobe eavesdropping using a 60 GHz testbed. The work in [9] presents an attack that exploits the weakness in the paging protocols used in 4G/5G to eavesdrop on the paging broadcast channel to infer the legitimate user's current cellular area. There exists several works in the literature that studies the coverage probability and secrecy performances of legitimate nodes in a mmWave cellular system. For example, [10] uses stochastic geometry to study the coverage probability of mmWave cellular systems. Cheng *et al.* [11], Yang *et al.* [12], Wildman *et al.* [13] study the impact of mmWave beam misalignment on the coverage probability. The work in [14] discusses secure connection probability for colluding and non-colluding eavesdropper in a multi-antenna system. The works in [10]–[14] are primarily to study the system performance of mmWave cellular systems and also they do not explicitly model the impact of ambient reflectors. While [7] focused on experimentally demonstrating eavesdropping in mmWave systems using a 60 GHz test bed, however, to our best knowledge, no existing work has provided an analytical model to characterize various eavesdropping attacks in 802.11ad mmWave WLANs.

The main objective of this paper is to develop an analytical model for the probability of successful eavesdropping under various attack scenarios. In this paper, we analyze the success possibility of two types of eavesdropping attacks, including the opportunistic stationary attack and the active nomadic attack. In the opportunistic stationary attack, the eavesdropper can only stay in the random position of the indoor environment. We consider when the LOS path is available and when only NLOS path is available due to reflectors. Stochastic geometry based success probability analysis is developed for the eavesdropper in the presence of LOS and reflected signal paths. In the active nomadic attack, the eavesdropper can move to any location in the environment to launch the attack. We first develop the LOS region estimation method based on the 802.11ad beam search procedure so that the eavesdropper knows where to move. Then the successful possibility of the active nomadic attack is derived. Finally, we evaluate our analytical model under various scenarios. We also perform eavesdropping experiments using commercially available 802.11ad devices [15] and a 60 GHz mmWave transceiver from VubiQ [16].

The main contributions of this work are summarized as below:

- We introduce two types of eavesdropping attack strategies: opportunistic stationary attack and active nomadic attack.
- We develop a tractable analytical model for success probability of eavesdropping under opportunistic stationary attack model considering both the LOS and the reflections from the environment. We also consider the errors introduced by beam searching procedures in our analytical model.
- Next, we for the first time develop the active nomadic attack strategy based on the localization of transmitter and receiver as well as the LOS region estimation. We provide the analytical model for success probability under active nomadic attack considering the LOS and the reflections from the environment. Similar to opportunistic stationary attack model, we consider the effect of errors introduced by the localization procedure on the success probability.
- We provide numerical analysis for both the proposed attacker scenarios. We discuss the effect of beamwidth and beam direction misalignment on the success probability of eavesdropping. We show that by leveraging on the 802.11ad beam searching procedure and ambient reflectors in the environment, with our proposed eavesdropping attacker strategies, Eve could potentially eavesdrop on legitimate pair of mmWave nodes with high probability.
- We also perform experiments using commercially available 802.11ad devices and transceivers to demonstrate our proposed opportunistic stationary attacker strategy and active nomadic attack strategy. We perform experiments in two different environments: 1. An indoor laboratory scenario and 2. Large atrium of a building. Experimental results compliment our results from analytical simulations.

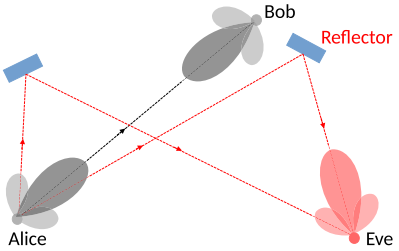


FIGURE 1. System model with alice, bob, eve and reflectors.

The remainder of this paper is structured as follows. In Section II, we introduce the system model and in Section III and Section IV, we present two eavesdropper attack strategies for 802.11ad WLAN systems and discuss the probability of successful overhearing of transmission under those strategies. In Section V, we analytically validate our proposed eavesdropper attacker models and also provide experimental results to support the analytical models. Section VI offers conclusions.

II. SYSTEM MODEL

In this section, we discuss our system model for our proposed eavesdropping attacker strategies. Fig. 1 depicts a generic eavesdropping scenario with Alice, Bob and Eve. Alice and Bob are legitimate users communicating using directional antenna following the 802.11ad protocol. Eve tries to eavesdrop on Alice communication to Bob and relies on the availability of LOS or reflected beam from an ambient reflector. We model this scenario using stochastic geometric approach. Before discussing the system model for our proposed attack strategies, we briefly describe the 802.11ad sector sweep protocol which is used to establish directional communication link between Alice and Bob. In this work, our proposed eavesdropping attacker strategies leverage on the 802.11ad sector sweep mechanism to eavesdrop on the legitimate pair of nodes. In contrast to the 2.4 GHz and 5 GHz WLAN systems which use single beacon for device discovery and management, 802.11ad uses beacon header interval (BHI). During the BHI, series of directional beacons are transmitted to facilitate network announcement and exchange of management informations. The directional beacons overcomes increased attenuation at high frequencies which is inherent to 60 GHz systems and also aids in discovery of unknown direction of unassociated devices. The BHI consists of three sub intervals namely beacon transmission interval (BTI), association beamforming training (A-BFT) and announcement transmission interval (ATI). The BTI consists of multiple beacon frames, each transmitted by the access point (AP) over different sectors. During the BTI period, the clients listen to these beacons from various sectors and choose the sector with highest RSSI/SNR as the sector to be used from AP to client direction. During the A-BFT period, the AP and the client interchange their roles. The client sweeps sector sweep frames, each in different sector. The AP listens to these sector sweep frames from the clients and in a similar fashion to BTI period, chooses the best sector from the client. The best sector ID from AP to client direction obtained by the client during the BTI period is piggybacked in all the sector sweep frames transmitted by the client. The best sector ID from client to AP obtained during the A-BFT period by the AP is communicated through explicit SSW feedback frame. Eve could passively listen to the beacon frames and obtain the sector ID's used between the legitimate pair of nodes.

A. GEOMETRIC ASSUMPTIONS

1) OBSTACLES AND REFLECTORS

Each object (obstacle or reflector) is of a shape specified by its center location C, length L, width W and orientation θ, where θ is the anti-clockwise angle between the x-axis and the length of the object. The centers $\{C\}$ of obstacle and reflector form a homogeneous Poisson Point Process (PPP) Φ with intensity λ. Certain fraction μ of the objects are obstacles and remaining are reflectors. Accordingly, the centers of the obstacles form a PPP Φ_o with density $\lambda_o = \mu\lambda$ and the centers of the reflectors form a PPP Φ_r with density $\lambda_r = (1-\mu)\lambda$. The lengths and widths of the obstacles and reflectors are assumed to be independent and identical distributions with PDF $f_L(l)$ and $f_W(w)$ respectively.

2) mmWAVE NODES

The spatial locations of the transmitters (access points) are modeled as homogeneous Poisson Point Process (PPP) Φ_n with intensity λ_n.

B. REFLECTION COEFFICIENT

The reflectivity of a surface depends on the properties of the material, angle of incidence, and the polarization of the incident wave. The reflection coefficients $\Gamma_\perp$ and $\Gamma_\parallel$ for a homogeneous dielectric plate with a smooth surface, thickness Δ, and complex refractive index n is given by [17] $\Gamma_l = \frac{1-e^{-2j\delta}}{1-\gamma_l^2 e^{-2j\delta}}\gamma_l, \quad l \in \{\perp, \parallel\}$ with $\delta = \frac{2\pi\Delta}{\lambda}\sqrt{n^2-\sin^2\theta}$, $\gamma_\perp = \frac{\cos\theta-\sqrt{n^2-\sin^2\theta}}{\cos\theta+\sqrt{n^2-\sin^2\theta}}$, and $\gamma_\parallel = \frac{n\cos\theta-\sqrt{n^2-\sin^2\theta}}{n\cos\theta+\sqrt{n^2-\sin^2\theta}}$. Where λ is the wavelength. The coefficients $\Gamma_\perp$ and $\Gamma_\parallel$ relate the reflected and the incident electric fields when the polarization is respectively perpendicular and parallel to the plane of incidence. We ignore the effect of roughness of the surface due to the fact that at millimeter wave frequencies, diffuse scattering off rough surfaces does not contribute significantly to the received signal power. The reflected paths follow specular reflection law and the diffraction paths are negligible as this propagation mechanism contributes to insignificant signal strength at mmWave bands [18], [19].

C. ANTENNA PATTERN

Millimeter wave nodes are capable of utilizing directional beamforming to overcome high path-loss incurred at 60 GHz [2]. In this work, we consider all the nodes to be equipped with an antenna array to perform beamforming. We consider two type of antenna beampattern model: (1) ideal

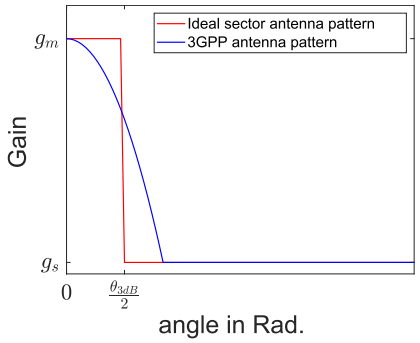


FIGURE 2. Comparison between the ideal sector antenna pattern and the 3GPP antenna pattern.

sectored antenna model and (2) 3GPP antenna model. Fig. 2 shows the antenna pattern of ideal sector antenna as well as the 3GPP antenna.

1) IDEAL SECTOR ANTENNA MODEL

For analytical tractability, many works in the literature [10], [20] approximated the actual antenna pattern with a sector antenna model to analyze the coverage probability of millimeter wave networks. The ideal sectored antenna model is parameterized by the mainlobe beamwidth θ_1, mainlobe gain g_m and sidelobe gain g_s. Ideal sector antenna has a constant gain g_m over the mainlobe beamwidth. The ideal sector antenna model is given by

$$G_{ideal}(\theta) = \begin{cases} g_m, & \text{if } |\theta| \leq \dfrac{\theta_1}{2}, \\ g_s, & \text{otherwise.} \end{cases} \tag{1}$$

2) 3GPP ANTENNA MODEL

The ideal sector antenna model in (1) has severe limitations in analyzing the impact of antenna pattern in the performance of millimeter wave networks in that it assumes constant antenna gain over the entire mainlobe beamwidth. For the antenna model in (1), misalignment between the transmitter and receiver antenna pattern has no impact on the received signal power. However, in practical scenarios, the reduction in the mainlobe gain due to such misalignment cannot be ignored. In this work, in addition to the ideal sector antenna model, to capture the practical beamforming errors in 802.11ad networks, we also consider 3GPP antenna model proposed in [21]. The 3GPP antenna pattern is given by

$$G_{3GPP}(\theta) = \begin{cases} g_m 10^{\frac{-3}{10}(\frac{2\theta}{\theta_{3dB}})^2}, & \text{if } |\theta| \leq \dfrac{\theta_1}{2}, \\ g_s, & \text{if } \dfrac{\theta_1}{2} \leq |\theta| \leq \pi. \end{cases} \tag{2}$$

where g_m and g_s are the mainlobe and sidelobe gains respectively. θ_{3dB} is the half-power beamwidth and $\frac{\theta_1}{2} = \frac{2.6\theta_{3dB}}{2}$ is the angle at which the mainlobe fall off to the sidelobe level.

D. BEAM DIRECTION ERROR MODEL

To model the effect of antenna alignment error in 802.11ad systems, we consider nodes to have a random antenna beam pattern misalignment denoted by θ_ϵ. We follow the beam misalignment error model proposed in [13] and [12]. Similar to the assumptions in [13] and [12], we assume beam pattern misalignment θ_ϵ is symmetric about the boresight angle θ and hence we consider absolute beam orientation error $|\theta_\epsilon|$ in our analysis. Since the beam searching procedure of 802.11ad aligns the main beam of the transmitter and receiver, it is less likely that the two beams are completely misaligned. Therefore in our work, we assume that the beam misalignment is likely to occur around the boresight. $|\theta_\epsilon|$ is bounded within the range of the mainlobe beam width θ_1. i.e., $0 \leq |\theta_\epsilon| \leq \frac{\theta_1}{2}$. Fig. 3 depicts the scenario where Eve's beam pattern is misaligned by θ_ϵ with respect to her boresight angle θ, and her corresponding antenna gain due to θ_ϵ is $G(\theta_\epsilon)$. When the beam pattern's are perfectly aligned, $\theta_\epsilon = \theta$ and Eve has a maximum antenna gain of $G(\theta)$. Among the distributions that satisfy the error model considered, we choose truncated normal distribution error model [13], [12], [22]. θ_ϵ follows truncated normal distribution with PDF given by

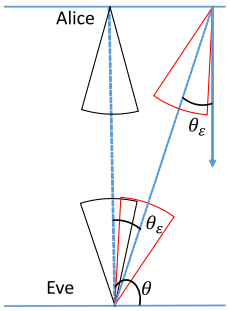


FIGURE 3. Antenna beam pattern misalignment θ_ϵ between alice and eve.

$$f_{\theta_\epsilon}(x) = \frac{e^{\frac{-x^2}{2\sigma_{\theta_\epsilon}^2}}}{\sigma_{\theta_\epsilon}\sqrt{2\pi}\, erf\left(\frac{\theta_1}{2\sqrt{2}\sigma_{\theta_\epsilon}}\right)} \tag{3}$$

where σ_ϵ^2 is the variance of the angle error.

E. ANTENNA GAIN DISTRIBUTION

Since the beam direction θ_ϵ is a random variable with PDF given by (3), the antenna gain $G(\theta_\epsilon)$ is also a random variable. We derive the antenna gain distribution for both ideal sector antenna pattern in (1) and 3GPP antenna pattern in (2).

1) 3GPP ANTENNA MODEL

Lemma 1: Let $f_{\theta_\epsilon}(x), |x| \leq \frac{\theta_1}{2}$ be the pdf of beam angle error θ_ϵ, then the antenna gain pdf $f_{g_{\theta_\epsilon}}(x)$ for $x \in [g_s, g_m]$ is given by

$$f_{g_{\theta_\epsilon}}(x) = \frac{\theta_{3dB} f_{\theta_\epsilon}(\theta_{3dB}\sqrt{(\frac{5}{6}log_{10}(\frac{g_m}{x}))})}{ln(10)x\sqrt{(\frac{6}{5}log_{10}(\frac{g_m}{x}))}}. \tag{4}$$

Proof: Proof is provided in Appendix A. □

2) IDEAL SECTOR ANTENNA

Let $f_{\theta_\epsilon}(x)$, $|x| \leq \frac{\theta_1}{2}$ be the pdf of beam angle error θ_ϵ, then the antenna gain pdf $f_{g_{\theta_\epsilon}}(x)$ for $x \in [g_s, g_m]$ is given by [13]

$$f_{g_{\theta_\epsilon}}(x) = \left(1 - F_{|\theta_\epsilon|}\left(\frac{\theta_1}{2}\right)\right)\delta(g_1) + F_{|\theta_\epsilon|}\left(\frac{\theta_1}{2}\right)\delta(g_2) \quad (5)$$

where $g_1 = g - g_s$ and $g_2 = g - g_m$.

F. CHANNEL MODEL

In this work, we consider the following path loss model for our mmWave system:

$$PL = A_1 log_{10}(d) + A_2 + A_3 log_{10}(f_c)\ (dB), \quad (6)$$

where d and f are the distance (meters) and carrier frequency (GHz), respectively. A_1, A_2, A_3 describes path loss exponent, intercept and the path loss frequency dependence.

For our analytical and experimental studies, we use path loss models from IEEE 802.11ad channel model document [23]. The LOS path loss is given by

$$PL_{LOS}(dB) = 32.5 + 20log_{10}(f_c) + 10n_{LOS}log_{10}(d) \quad (7)$$

respectively. We assume $n_{LOS} = 2$ for indoor millimeter wave scenarios [23], [24].

Due to the properties of mmWave propagation, multi-path effects are negligible [25]. For example, at 60 GHz, the channel closely matches an Additive White Gaussian Noise (AWGN) channel [25]. Consequently, we do not consider multi-path fading in our mmWave channel model. We consider a noise-limited 60 GHz mmWave WLAN system and the signal-to-noise ratio (SNR) at a receiver is given by $SNR = \frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(A)d^\alpha\sigma^2\rho}$, where P_{tx} is the transmit power, $G_{tx}(\theta)$ is the antenna gain of transmitter, $G_{rx}(\theta)$ is the antenna gain of receiver, d is the distance between transmitter and receiver, α is the path loss exponent and σ^2 is the noise variance. For the NLOS path, ρ is the reflection coefficient of the reflector and it depends on the reflecting material and for the LOS path $\rho = 1$.

G. DISTANCE DISTRIBUTION

Let R_0 denote the distance between the transmitter and a receiver. Let λ_n denote the intensity of the transmitters. The PDF of the random variable R_0 between the transmitter and the receiver is given by the following lemma.

Lemma 2: The PDF $f_{R_0}(r)$ and CDF $F_{R_0}(r)$ of the random variable R_0 is given by

$$f_{R_0}(r) = 2\pi\lambda_n r e^{-\beta_o r + p + 2\pi\lambda\frac{e^{-p}}{\beta_o^2}[1-(\beta_o r+1)e^{-\beta_o r}]} \text{ and}$$
$$F_{R_0}(r) = 1 - e^{-2\pi\lambda_n\frac{e^{-p}}{\beta_o^2}[1-\beta_o r e^{-\beta_o r} - e^{-\beta_o r}]}, \quad (8)$$

respectively. Where $\beta_o = \frac{2\lambda(\mathbb{E}[L]+\mathbb{E}[W])}{\pi}$ and $p = \lambda\mathbb{E}[L]\mathbb{E}[W]$.

Proof: The proof can be found in [26]. □

The main notations used in the paper are summarized in Table. 1.

TABLE 1. List of main notations and definitions.

Notation	Description
Φ_n, Φ	PPPs of transmitters and obstacles
$\lambda_n, \lambda_o, \lambda_r$	Intensities of transmitters, obstacles, and reflectors
ρ	Reflection coefficient of reflectors
P_{tx}, P_{rx}	Transmit power of Alice and receive power of Eve
$G_{ideal}(\theta), G_{3GPP}(\theta)$	Ideal and 3GPP antenna gain pattern
$G_{tx}(\theta), G_{rx}(\theta)$	Antenna gain patterns of the transmitter (Alice) and receiver (Eve)
β	SNR threshold
θ_ϵ	Beampattern alignment error
$f_{\theta_\epsilon}(x)$	PDF of the beampattern alignment error
$f_{G_{rx}(\theta)}(x)$	PDF of receive antenna gain pattern
L, W	Length and width of the obstacles and reflectors
r_1, r_2	Distance of the reflector to Alice and distance of the reflector to Eve
$F_d(x)$	CDF for the eavesdropper link with distance d
$P(LOS_{Eve}), P(Ref_{Eve})$	Probability Eve is covered by LOS and probability Eve is covered by reflection
P_{LOS}, P_{Ref}	Probability of LOS path and probability of reflected path
$P(C_{Eve})$	Overall eavesdropping success probability

III. OPPORTUNISTIC STATIONARY ATTACKER

In the opportunistic stationary attack model, depending on Eve's random location, Eve could overhear Alice's transmission either through LOS signal or through reflections from the reflectors. In this mode of attack, Eve does not move her position. She stays in her random location and her success of overhearing Alice's transmission heavily depends on the availability of LOS or reflections from the environment. Initially Eve uses directional antenna and continuously scan the environment for the best possible reception from Alice. Eve steps through her beampatterns sequentially and decides on the beampattern with highest RSSI/SNR from Alice to overhear. The best direction or sector for Eve could be a LOS or NLOS link. Eve periodically sweeps the environment to update her best sector to overhear Alice to Bob communication. The probability of Eve for successfully overhearing Alice's communication depends on the LOS or NLOS link between Alice and Eve. Accordingly, in the subsequent sections we derive the LOS and NLOS success probability for Eve under opportunistic attacker model.

A. SUCCESS PROBABILITY ANALYSIS

Let SNR_{Eve} denote the signal-to-noise ratio obtained at the eavesdropper due to LOS or reflected signal. β denotes the SNR threshold at which Eve can successfully overhear the signal from the transmitter Alice. Due to the random distributions of the objects in the indoor environment under consideration, the eavesdropper could be covered by either direct LOS signal from Alice or through the reflections from the ambient reflectors in the indoor environment. Accordingly P_{LOS} and P_{ref} denote the coverage probability of Eve due to LOS and reflected signals, respectively.

We define $C_{Eve} : SNR_{Eve} \geq \beta$ as the event when the received SNR of Eve is above a certain threshold to successfully receive the signal. Accordingly, the probability that Eve will be able to successfully receive Alice's signal is given by

$$P(C_{Eve}) = P(SNR_{Eve} \geq \beta). \tag{9}$$

We further define two events LOS_{Eve} and Ref_{Eve} as the events when the eavesdropper is covered by a LOS signal from the legitimate transmitter Alice and by reflections from the reflectors present in the environment, respectively. Since the contributions of second-order and higher-order reflections to the total received signal power are negligible in mmWave systems, in our system model we only consider first-order reflections. We further make assumptions that the reflected signal is fully reflected by the obstacle with reflection co-efficient ρ. We also ignore refraction and diffraction of signals in our system model [18], [19]. By taking into account the possibility of Eve being covered by either LOS from Alice or by reflections from the environment, the coverage probability of Eve is given by

$$\begin{aligned} P(C_{Eve}) = {} & P(SNR_{Eve} \geq \beta | LOS_{Eve}) P(LOS_{Eve}) \\ & + P(SNR_{Eve} \geq \beta | Ref_{Eve}) P(Ref_{Eve}). \end{aligned} \tag{10}$$

B. LINE OF SIGHT SUCCESS PROBABILITY

Since we have modeled obstacles and reflectors present in the environment as a PPP, the total number of obstacles N between Alice and Eve separated by distance d is a Poisson random variable with mean $\beta_o d + p$ [26]. In our work, we consider the height at which the transmitter and receiver are placed as typically in an indoor environment they are not placed at the same height. In our model, the object height $H_i \in [H_{min}, H_{max}]$ are modeled with pdf $f_H(h)$. Let H_{tx} and H_{rx} denote the height at which the transmitter and the receiver antennas are located. The probability that there exist a LOS link between Alice and Eve with distance d, i.e., there are no obstacles between them is given by [26]

$$P_{Los} = e^{-\eta(\beta_o d + p)}, \tag{11}$$

where $\beta_o = \frac{2\lambda(\mathbb{E}[L]+\mathbb{E}[W])}{\pi}$, $p = \lambda \mathbb{E}[L]\mathbb{E}[W]$, and $\eta = 1 - \int_0^1 \int_{H_{min}}^{sH_{rx}+(1-s)H_{tx}} f_H(h) dh ds$.

Therefore the probability Eve will be in LOS with respect to Alice is given by $P(LOS_{Eve}) = e^{-\eta(\beta_o d + p)} \overline{P}_{Ref}$. P_{Ref} is derived in Section III-C. Therefore, the success probability due to LOS is given by

$$\begin{aligned} & P(SNR_{Eve} > \beta | LOS_{Eve}) P(LOS_{Eve}) \\ & = \mathbb{E}_{G_{rx}(\theta)} \left[P\left(\frac{\alpha}{d^2} > \beta | LOS_{Eve} \right) \right] P(LOS_{Eve}) \\ & = \mathbb{E}_{G_{rx}(\theta)} \left[P\left(d < \sqrt{\frac{\alpha}{\beta}} \right) \right] P(LOS_{Eve}) \\ & = \int_{g_r} F_d(x) \Big|_{x=\sqrt{\frac{\alpha}{\beta}}} P(LOS_{Eve}) f_{G_{rx}(\theta)}(g_r) \mathrm{d}g_r \end{aligned} \tag{12}$$

where $F_d(x)$ is given by (8) and $\alpha = \frac{P_{tx} G_{tx}(\theta) G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2 \sigma^2}$.

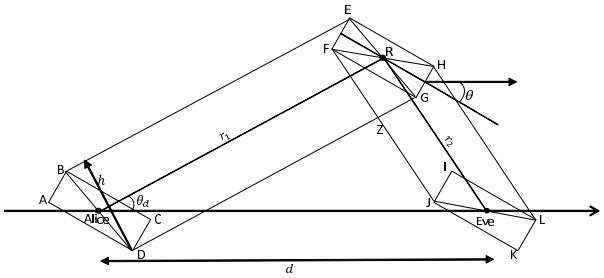


FIGURE 4. Blockage region for the reflected path [27].

C. REFLECTION SUCCESS PROBABILITY

In this section we discuss the success probability of Eve due to the reflectors in the environment.

The reflector orientation θ is modeled as uniform distribution with density $f_\Theta(\theta) \sim U(0, \pi)$. The center of each reflector is generated from a PPP with density λ_r. The blockage analysis for the reflected path is similar to the one proposed in [26]. Suppose that there exists a reflector with center at R that can potentially generate reflection path to the receiver. Therefore this reflection path has two segments Alice-R and R-Eve. For this reflector with center R to potentially contribute to the reflection path to Eve, there must not be blockage in the area formed by $ABEHLKJZD$ as shown in Fig. 4. Let the area of the region $ABEHLKJZD$ is denoted by $S(L, W, \theta)$. Then from [27], $S(L, W, \theta) = (r_1 + r_2)h + LW - \frac{L((r_1+r_2)-d)}{4} - \frac{L^2\sqrt{((r_1+r_2)^2-d^2)}}{8d}$. Let $N(L, W, \theta)$ be the number of blockages that fall within the area $ABEHLKJZD$. $N(L, W, \theta)$ is a Poisson random variable with expectation $\mathbb{E}[N(L, W, \theta)] = \lambda_o S(L, W, \theta)$. For any realizations of obstacles, the mean number of obstacles falling within the region $ABEHLKJZD$ is $N = \sum_{L,W,\theta} N(L, W, \theta)$. N is Poisson distributed and its expectation is given by [27]

$$\begin{aligned} \mathbb{E}[N] = {} & \int_L \int_W \mathbb{E}[N(L, W, \theta)] f_W(w) f_L(l) \mathrm{d}W \mathrm{d}L \\ = {} & \lambda_o \Bigg(\mathbb{E}[L] \sqrt{(r_1 + r_2)^2 - d^2 cos^2\theta} + \mathbb{E}[W] d \\ & + \mathbb{E}[L]\mathbb{E}[W] - \frac{\mathbb{E}[L](r_1 + r_2 - d)}{4} \\ & - \frac{\mathbb{E}[L]^2 \sqrt{(r_1 + r_2)^2 - d^2}}{8d} \Bigg). \end{aligned} \tag{13}$$

The probability P_{Ref} that the reflector with center at R and reflected path $Alice - R - Eve$ is unobstructed and serves as a NLOS to Eve is given by the following lemma.

Lemma 3: The probability of reflected path for a reflector with center at R and at a distance r_1 from Alice and at a distance r_2 to Eve is given by

$$P_{Ref} = e^{-\lambda_o \left(\mathbb{E}[L]A + \mathbb{E}[W]B + \mathbb{E}[L]\mathbb{E}[W] - \mathbb{E}[L]C - \mathbb{E}[L]^2 D \right)}, \tag{14}$$

with $A = \sqrt{(r_1 + r_2)^2 - d^2 cos^2\theta}$, $B = d$, $C = \frac{(r_1+r_2-d)}{4}$, *and* $D = \frac{\sqrt{(r_1+r_2)^2-d^2}}{8d}$.

Proof: The proof is given in Appendix B. □

1) DISTRIBUTION OF THE DISTANCE TO THE REFLECTOR

Having discussed the probability of the availability of reflected path to Eve, next we discuss the distribution of the distance of Eve from the reflector. As mentioned before, the reflectors are distributed according to a PPP of density λ_r. The CDF of the distance r_2 to the closest reflector is similar to the analysis in Section II-G and is given as

$$F_{r_2}(r) = 1 - e^{-2\pi\lambda_r \frac{e^{-p}}{\beta_o^2}[1-\beta_o r e^{-\beta_o r} - e^{-\beta_o r}]} \tag{15}$$

where $\beta_o = \frac{2\lambda(\mathbb{E}[L]+\mathbb{E}[W])}{\pi}$ and $p = \lambda\mathbb{E}[L]\mathbb{E}[W]$.

Therefore, the success probability of Eve due to reflections from the environmental reflectors is given by

$$\begin{aligned} P(SNR_{Eve} > \beta | Ref_{Eve}) P(Ref_{Eve}) &= \mathbb{E}_{G_{rx}(\theta)}\left[P\left(\frac{\alpha}{r_2^2\rho} > \beta | Ref_{Eve}\right)\right] P(Ref_{Eve}) \\ &= \mathbb{E}_{G_{rx}(\theta)}\left[P\left(r_2 < \sqrt{\frac{\alpha}{\beta\rho}}\right)\right] P(Ref_{Eve}) \\ &= \int_{g_r} F_{r_2}(r)\Big|_{r=\sqrt{\frac{\alpha}{\beta\rho}}} P(Ref_{Eve}) f_{G_{rx}(\theta)}(g_r)\mathrm{d}g_r \end{aligned} \tag{16}$$

where $F_{r_2}(r)$ is given by (15), $P(Ref_{Eve}) = P_{Ref}\overline{P}_{Los}$ and $\alpha = \frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2\sigma^2}$.

The success probability for Eve under opportunistic stationary attack strategy is given by the Corollary 1.

Corollary 1: Given an SNR threshold T, the success probability of Eve under opportunistic stationary attack model is given by (17)*, as shown at the bottom of this page, where $F_d(x)$ is given by* (8)*, $F_{r_2}(x)$ is given by* (15)*, and $f_{G_{rx(\theta)}}(g_r)$ is the PDF of the antenna gain which takes the form in (4) for 3GPP antenna model and (5) for ideal sector antenna model.*

Since under opportunistic stationary attack strategy, Eve randomly chooses a location in the environment to eavesdrop on Alice's transmission, Corollary 1 shows that, the success probability for Eve depends on the availabilty of LOS link with respect to Alice as well as the reflections enabled by the ambient reflectors in the environment. Also from (17), the success probability of Eve due to reflections depend on the density of the reflector λ_r, density of obstacles λ_o, and the distance r_2 of Eve from the reflector. When the environment has many reflectors which is typically the case for indoor scenarios and when Eve is at a distance $r_2 \leq \sqrt{\frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2\beta\sigma^2\rho}}$ from a potential reflector, even when Eve is not in the LOS region of Alice, she could still be able to listen to transmissions from Alice owing to the reflectors present in the environment.

IV. ACTIVE NOMADIC ATTACKER

In this section, we describe the active nomadic attack strategy for eavesdropping Alice's communication to Bob. In contrast to the opportunistic stationary attacker strategy described in Section III, in active nomadic attacker strategy Eve takes full advantage of the beam searching protocol of 802.11ad and has the capability to estimate the LOS region between Alice to Bob communication and move to a desired location in the estimated LOS region. The proposed active nomadic attack strategy leverages on the sector sweep process between Alice and Bob and is outlined as follows.

A. LOCALIZATION PROCEDURE

Alice and Bob uses sector sweep mechanism of 802.11ad to find the respective best sector based on the received signal power or SNR to establish directional communication between them. These sector sweep frames are transmitted in the BTI and A-BFT period of the beacon interval. Eve from a random location, periodically listens to these beacons using omni-directional antenna. In order to estimate the active communication sector A between Alice and Bob and move to the estimated sector, Eve must first estimate Alice's position. The location of Alice can be estimated from the 802.11ad beam searching protocol outlined in Section II. Let $S = \{s_1, s_2, \ldots, s_n\}$ denote the set of sectors Alice uses in its beam searching protocol. The number of sectors n depends on the manufacturer and typically for an AP it varies from 32 to 36. TALON AD7200 router [15], for example uses 36 sectors in its beam searching procedure. Alice sends beacons in each of the n sectors every t ms. For e.g., the TALON AD7200 router sends beacon every 100 *ms*. Eve listens to these periodic beacons from Alice and selects the sector that gives maximum RSSI/SNR, denoted as s_0, as the sector direction in which Alice is located. s_0 is the localization sector of Alice. The angle α_A of Alice direction is determined with

$$\begin{aligned} P(C_{Eve}) = &\int_{g_r}\left[F_d(x)\right]_{\sqrt{\frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2\beta\sigma^2}}} e^{-\eta(\beta_o d+p)} \\ &\times\left(1 - e^{-\lambda\left(\mathbb{E}[L]\sqrt{(r_1+r_2)^2-d^2\cos^2\theta}+\mathbb{E}[W]d-\mathbb{E}[L]\mathbb{E}[W]-\frac{\mathbb{E}[L](r_1+r_2-d)}{4}-\frac{\mathbb{E}[L]^2\sqrt{(r_1+r_2)^2-d^2}}{8d}\right)}\right) f_{G_{rx}(\theta)}(g_r)dg_r \\ &+\int_{g_r}\left[F_{r_2}(x)\right]_{\sqrt{\frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2\beta\sigma^2\rho}}} e^{-\lambda\left(\mathbb{E}[L]\sqrt{(r_1+r_2)^2-d^2\cos^2\theta}+\mathbb{E}[W]d+\mathbb{E}[L]\mathbb{E}[W]-\frac{\mathbb{E}[L](r_1+r_2-d)}{4}-\frac{\mathbb{E}[L]^2\sqrt{(r_1+r_2)^2-d^2}}{8d}\right)} \\ &\times(1 - e^{-\eta(\beta_o d-p)}) f_{G_{rx}(\theta)}(g_r)\mathrm{d}g_r. \end{aligned} \tag{17}$$

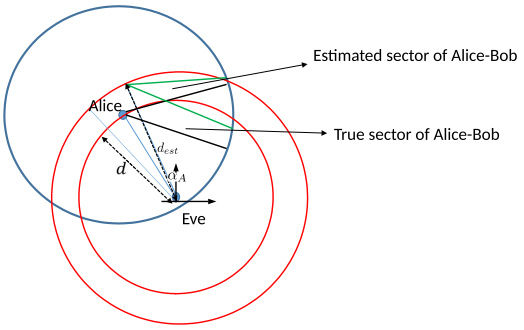


FIGURE 5. Uncertainty in estimating alice position.

respect to Eve's position as shown in Fig. 5. It is assumed that Eve knows her own 0° orientation. α_A is the angular offset from Eve's 0° orientation and the center of Alice to Eve localization sector s_0. Because of beam misalignment in practical mmWave systems, the direction of Alice may not be the angle α_A the center of localization sector s_0 makes with Eve's 0° orientation. As per our beam direction error model, this random beam misalignment is denoted as θ_ϵ. Since the active nomadic attack strategy relies on the sector sweeping procedure of the 802.11ad protocol for estimating Alice direction, the accuracy of direction estimation heavily depends on the best sector Eve finds to Alice. Upon finding the direction of Alice from her, Eve from the measured RSSI of the beacon corresponding to the decided sector, estimates the distance between her and Alice using the channel model in Section II-F. The distance of Alice form Eve is a random variable because of the uncertainty in estimating the direction of Alice. Based on the indoor mmWave path loss model discussed in Section II-F and with the knowledge of transmit power of Alice, the distance to Alice can be estimated as

$$d_{est} = \sqrt{\frac{P_{tx}G_{tx}(\theta)}{(\frac{4\pi}{\lambda})^2 P_{rx}}}\sqrt{(G_{rx}(\theta))}. \tag{18}$$

From (18), we see that the distance estimation is influenced by the antenna gain. Therefore, the estimated distance between Alice and Eve is modeled as a random variable.

Lemma 4: Given an antenna alignment error θ_ϵ, the CDF of the distance estimation between Alice and Eve is given by,

$$F_{d_{est}}(x) = F_{G_{rx}(\theta_\epsilon)}\left(\frac{x^2(\frac{4\pi}{\lambda})^2 P_{rx}}{P_{tx}G_{tx}(\theta)}\right) \tag{19}$$

Proof: The proof is given in appendix C. □

Eve with the knowledge of the direction and the distance of Alice from her, the next step is to determine the sector with which Alice communicates with Bob. Similar to the direction estimation between Alice and Eve, the sector between Alice and Bob could be found through the SSW frames transmitted by Bob to Alice. The SSW frames from Bob of the A-BFT period contains a field with the best sector ID found from the beaconing from Alice during the BTI period. Eve listens to these SSW frames and extracts the sector ID from them. Now with the knowledge of estimated Alice position and the sector ID between Alice and Bob, Eve estimates the sector region of communication between Alice and Bob and moves to the estimated region. (θ_{Eve}, r_{Eve}) is the position of Eve in the estimated region. Alice to Bob estimated sector boundary is defined by the parameters $[\theta_{est} - \frac{\theta_1}{2}, \theta_{est} + \frac{\theta_1}{2}]$ and d_{max}, where θ_{est} is the estimated sector angle between Alice and Bob based on the sector ID and θ_1 is the mainlobe beamwidth of Alice's antenna pattern, which is assumed to be known to Eve. d_{max} is the maximum coverage region of Alice centered at (α_A, d_{est}). d_{max} is known from the EIRP of Alice, the channel model adopted and the minimum SNR required by Eve for reliable eavesdropping.

B. DISTANCE DISTRIBUTION OF THE LINK BETWEEN ALICE AND EVE

An important parameter in the success probability of Eve under active nomadic attack is the distance R between Alice and Eve once Eve moves to the estimated sector between Alice and Bob. For the Alice to Bob communication sector region A, the probability Eve is at a distance R is given by $P(R \leq r) = \frac{r^2}{d_{max}^2}$. Under active nomadic attack scenario, after estimating the sector between Alice and Bob, strategy for Eve is to move to a location R from Alice close to the maximum coverage range d_{max} i.e $r_{min} \leq R < d_{max}$. r_{min} and d_{max} can be found by the path loss model and SNR threshold required by Eve for reliable eavesdropping.

C. SUCCESS PROBABILITY ANALYSIS

In this section, we discuss the success probability of Eve with active nomadic attack strategy. The probability of Eve successfully overhearing Alice's transmission depends on the ability of Eve estimating the active communication sector between Alice and Bob and also by any reflections of Alice signal reaching Eve due to the ambient reflectors in the environment. Also, the success probability of Eve is greatly influenced by her beampattern orientation with respect to Alice. Accordingly, let R_1 denote the event Eve is in LOS of Alice and $\bar{R}_1$ denote the event Eve is covered by a reflector. The success probability of Eve is given by

$$\begin{aligned} P_{success} &= P(SNR > \beta) \\ &= P(SNR > \beta, R_1) + P(SNR > \beta, \bar{R}_1). \end{aligned} \tag{20}$$

The SNR CCDF of Eve conditioned on the event she is in the LOS of Alice is given by

$$\begin{aligned} &P(SNR > \beta, R_1) \\ &= P\left(R < \left(\frac{P_{Tx}G_{Tx}(\theta)G_{Rx}(\theta)}{\beta\left(\frac{4\pi}{\lambda}\right)^2\sigma^2}\right)^{\frac{1}{2}}\right) \\ &= \mathbb{E}_{G_{Rx}(\theta)}\left[P\left(R < \left(\frac{P_{Tx}G_{Tx}(\theta)G_{Rx}(\theta)}{\beta\left(\frac{4\pi}{\lambda}\right)^2\sigma^2}\right)^{\frac{1}{2}}\right)\right] \\ &= \int_{g_r}[F_R(r)]_{r=\sqrt{\frac{P_{Tx}G_{Tx}(\theta)G_{Rx}(\theta)}{\beta\left(\frac{4\pi}{\lambda}\right)^2\sigma^2}}} f_{G_{Rx}(\theta)}(g)\mathrm{d}g \end{aligned} \tag{21}$$

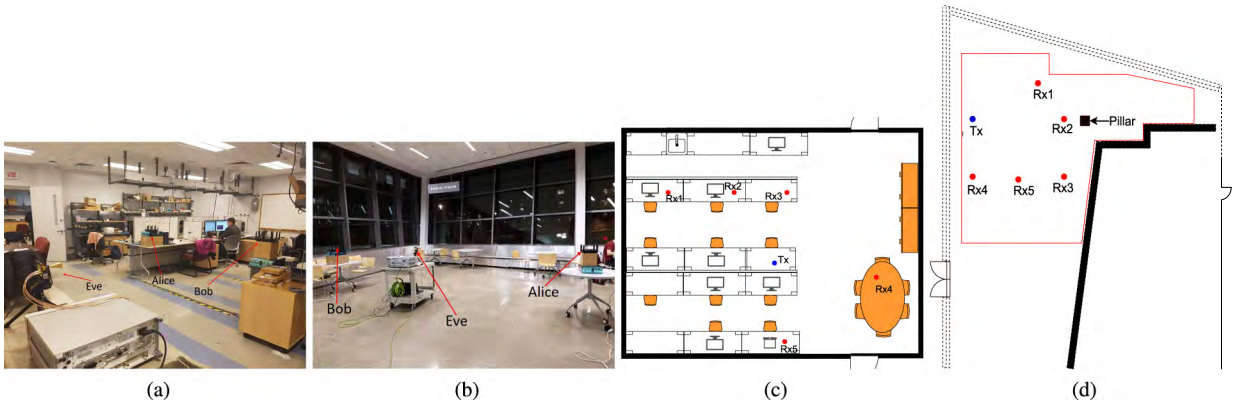


FIGURE 6. Experimental setup and floor plan of two different environments: (a) Laboratory; (b) atrium; (c) laboratory floor plan; (d) atrium floor plan.

where $F_R(r) = \frac{r^2}{d_{max}^2}$ and $f_{G_{Rx}(\theta)}$ is (4) for 3GPP antenna model and (5) for ideal sector antenna model.

The success probability of Eve due to reflectors $P(SNR > \beta, \bar{R}_1)$ is similar to Section III-C. Therefore the probability of Eve to successfully eavesdrop on Alice transmission is given by the following Corollary 2.

Corollary 2: Given a SNR threshold β, the success probability of Eve to overhear Alice transmission is given by (22), *as shown at the bottom of this page,*

where $f_{G_{rx}(\theta)}$ is (4) for 3GPP antenna model and (5) for ideal sector antenna model.

From Corollary 2, with active nomadic attack strategy, the ability of Eve to overhear Alice transmission depends on Eve's capability to estimate the LOS sector between Alice and Bob. Eve's success probability also depends on the beamwidth θ_1 of Alice antenna beam pattern. Wider the beam used by Alice, higher will be the probability that Eve's localization procedure results in her being in the correct sector served by the beam. For narrower beams, localization error in estimating the sector between Alice and Bob will result in Eve's gain being drastically reduced. In the worst case, localization error could result in Eve being in the adjacent sector than the actual communication sector between Alice and Bob. Also, it should be noted that, similar to opportunistic stationary attacker strategy, Eve's success probability under active nomadic attack strategy is enhanced by reflections from the environment. With active nomadic attack strategy, the ability for Eve to overhear Alice transmission to Bob is significantly improved, since Eve with 802.11ad beam searching protocol estimates the active sector of communication between Alice and Bob and directly moves to the region.

V. NUMERICAL ANALYSIS AND EXPERIMENTAL RESULTS

A. TESTBED AND EXPERIMENTAL SCENARIOS

In this section we describe our experimental scenarios to validate the proposed eavesdropping attacker strategies. Our numerical analysis also follows the same system and environment settings. Our experimental set up consists of three 60 GHz millimeter wave nodes Alice, Bob and Eve. All the three nodes use 802.11ad protocol for communication. We use TP-Link Talon AD7200 [15] routers as Alice and Bob. The router is equipped with 802.11ad QCA9008-SBD1 module with QCA 9500 chipset from Qualcomm. The router has a 32 element phased array antenna for directional communication using 802.11ad protocol. Alice is configured as an AP and Bob as a client. To implement the eavesdropping attacker protocols described in Section III and Section IV, an 802.11ad 60 GHz Acer Travelmate P446-M [28] laptop is used as eavesdropper (Eve). The laptop has a client version of the module QCA9008-TBD1. The laptop is equipped with the same 32 element phased array antenna that is used in TP-Link Talon AD7200 routers. The laptop uses Wilocity wil6210 wireless driver. Eve is configured to operate in *monitor* mode using the Wilocity driver to listen to the 802.11ad beacons and sector sweep frames from Alice and Bob. However, the Wilocity firmware does not provide signal strength measurements for the data packets overheard between Alice and Bob. Hence, the received signal power at Eve due to eavesdropping Alice to Bob communication is measured using a separate 60 GHz receiver from VubiQ [16]. The down-converted baseband signal from Vubiq is connected to a CXA N9000A signal analyzer to measure the signal power. We deploy our experimental set

$$P(C_{Eve}) = \mathbb{1}((\theta_{Eve}, r_{Eve}) \in A) \int_{g_r} [F_R(r)]_{r=\sqrt{\frac{P_{Tx}G_{Tx}(\theta)G_{Rx}(\theta)}{\beta\left(\frac{4\pi}{\lambda}\right)^2\sigma^2}}} f_{G_{rx}(\theta)}(g)dg$$

$$+ \mathbb{1}((\theta_{Eve}, r_{Eve}) \notin A) \int_{g_r} \left(1 - e^{-2\pi\lambda\frac{e^{-p}}{\beta_o^2}\left[1-\left(\beta_o\sqrt{\frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2\beta\sigma^2\rho}}+1\right)e^{-\beta_o\sqrt{\frac{P_{tx}G_{tx}(\theta)G_{rx}(\theta)}{(\frac{4\pi}{\lambda})^2\beta\sigma^2\rho}}}\right]}\right) f_{G_{rx}(\theta)}(g_r)\mathrm{d}g_r. \quad (22)$$

TABLE 2. Common parameters used in the simulation.

Parameters	Indoor
Carrier Frequency (GHz)	60.48
Bandwidth (MHz)	2310
Path Loss α	2
Uniform obst. height H (m)	[0,1]
Uniform obst. width W (m)	[0,1]
Uniform obst. length L (m)	[0,1]
Transmit EIRP (dBi)	24

up in two different environments. The first is a laboratory environment shown in Fig. 6a. The size of the laboratory is $8.5m \times 9$ m. This scenario includes cubicles, tables, chairs, and desktop monitors. Experiments were conducted during office hours with human mobility that introduces blockages. The floor plan is shown in Fig. 6c. The second is an atrium with glass panels on two sides of the atrium as depicted in Fig. 6b and the floor plan is shown in Fig. 6d. The atrium scenario is largely an open space with limited obstructions. In both the scenarios, the AP is deployed such that it provides best coverage to Bob. The experiments in the atrium were conducted with limited human mobility.

B. EVALUATION ENVIRONMENT

In this section we describe our numerical evaluation methodology and experimental validation methodology of our proposed eavesdropper attack strategy discussed in Section III and Section IV. We used MATLAB to analytically evaluate our proposed eavesdropper attacker strategies. Our system model consists of Alice and Bob which are legitimate node pairs communicating and an eavesdropper Eve. Alice and Bob uses 802.11ad based mmWave narrow beam communications for communicating with each other. Eve tries to overhear transmissions from Alice using LOS if available or through reflections from environmental reflectors. It is assumed that Alice and Bob completes beam searching procedure as per 802.11ad protocol and their beams are perfectly aligned. We also assume that Eve has the same capability as that of Alice and Bob and uses 802.11ad protocol. Locations of Alice, Bob and Eve are randomly chosen in the area. The obstacles and reflectors are randomly dropped following the PPP model discussed in Section II. The dimensions of the obstacles and reflectors are chosen to depict furnitures, fixtures and other objects found in a common indoor living room scenario. A list of common parameters used for the analytical validation are shown in Table 1. The carrier frequency and bandwidth are chosen to match with the carrier frequency and bandwidth used by the commercial devices in our experimental validation. The reflection loss ρ due to reflectors present in the environment is uniformly chosen between 2 dB and 23 dB [29].

1) mmWAVE NODE DISTRIBUTION

For the analytical evaluations, we consider an evaluation area of $8.5m \times 9$ m depicting an indoor living room as specified in TGad evaluation methodology document. For our

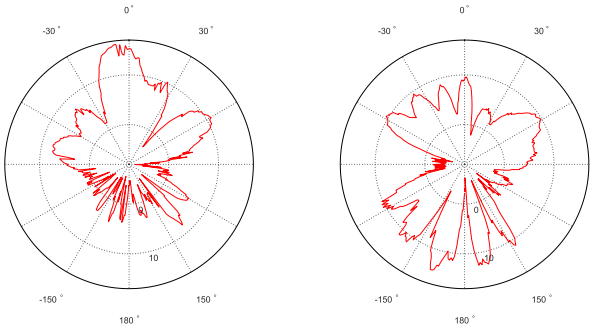


FIGURE 7. Measured sector patterns of TALON AD7200 [31]. (a) Sector 20. (b) Sector 30.

experiment, five different position configurations are used for Alice and Bob. In all the five configurations, the position of Alice which is referred to as *Tx* in the floor plan in Fig. 6c and Fig. 6d is fixed as is the case in most practical scenarios where the position of AP is usually fixed. Five positions are chosen for Bob which is referred to as *Rxi* with *i* specifying configuration index as shown in the Fig. 6c and Fig. 6d. The position of Eve is randomly chosen in the experimental area for each experiment.

2) ANTENNA CONFIGURATIONS

For the analytical studies, we assume Alice, Bob and Eve are equipped with directional antenna for communication. We consider two types of antenna model as described in Section II-C. For both the ideal sector antenna in (1) and 3GPP antenna model in (2), the main lobe gain, side lobe gain and antenna beam width are chosen as 24 dBi, 3 dBi and 30°, respectively for Alice unless otherwise specified. The mainlobe gain and beamwidth for the analytical studies are set according to the specifications of the commercial devices used in our experiments. The TALON AD7200 router which is used as Alice in our experiments has an EIRP of 24 dBi. The beamwidth for the TALON AD7200 is unspecified in the data sheet [30]. The work in [31] experimentally measures the antenna pattern of all the sectors used by TALON AD7200. From Fig.7, we see the TALON AD7200 routers antenna pattern is largely irregular without well defined notion of beamwidth and it varies roughly from 30° to 60°. Therefore, for our analytical studies we choose 30° beamwidth for Alice unless otherwise specified. The antenna gain and beamwidth of Eve is set as 24 dBi and 12° to match with the WR-15 standard gain horn antenna [32] used by the Vubiq 60 GHz receiver [16] which is used as Eve in our experiments. In the experiments, the antenna pattern used by Alice and Eve are determined by the 802.11ad beam searching protocol.

C. OPPORTUNISTIC STATIONARY ATTACK

In this section, we discuss the simulation and experimental results for opportunistic stationary attacker model discussed in Section III. Fig. 8 shows the success probability versus SNR for opportunistic stationary attacker model. Fig. 8

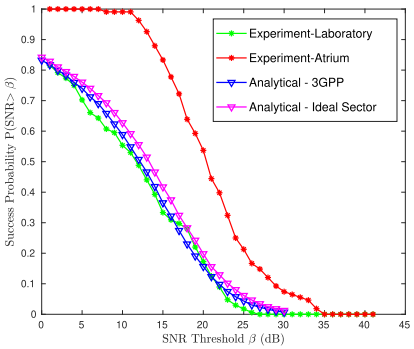


FIGURE 8. Success probability versus SNR threshold β for simulation and experiments in the laboratory and in the atrium.

compares the success probability obtained through analytical model and experiments in the Atrium and laboratory environment. The success probability is evaluated for both the ideal sector antenna pattern in (1) as well for the 3GPP antenna pattern in (2). For the analytical model, the antenna pattern of Eve is aligned to the best sector Eve sees from Alice. The simulations were carried for 10000 trials for each SNR threshold β and the average success probability is plotted for different SNR thresholds. From Fig. 8, it is seen that since the ideal sector antenna model uses constant gain over the entire mainlobe, the success probability with ideal sector antenna is higher than the success probability with 3GPP antenna pattern. The eavesdropper has higher probability to align its beam with ideal sector antenna than with 3GPP antenna model. Fig. 8 also shows the experimental success probability in the laboratory environment as well as in the atrium. In the atrium cases, it is observed that the experimental success probability is higher than the analytical success probability due to the fact that the antenna pattern used by commercial 60 GHz 802.11ad routers like TALON AD7200 and 802.11ad laptops have irregular beampattern and much higher sidelobes which results in many strong reflected paths. Also, the atrium scenario did not have any obstacles and Eve always has clear LOS to either the side lobes or to the reflectors in the atrium. Fig. 7a and Fig. 7b shows two of the actual measured sector patterns used by the TALON AD7200 routers [31]. Antenna pattern used by sectors 20 and 30 have very significant sidelobes that are as strong as the mainlobe. For example, antenna pattern used by sector 30 has significantly comparable gains in 60°, 170°, −60°, −120°, −140°, −165° directions. When Alice uses this sector for transmission to Bob, even if Eve is not in the LOS of Alice to Bob communication, has higher probability to eavesdrop on Alice transmission due to the significant sidelobes and reflections from Alice antenna pattern.

1) EFFECT OF ALICE'S ANTENNA

In the opportunistic stationary attacker model, Eve's probability of eavesdropping Alice's transmission significantly increases with the increase in the beamwidth of Alice beam pattern. Fig. 9a and Fig. 9b shows Eve's success probability for antenna beamwidths 3°, 7°, 10°, 20°, 30°, 40°, 50°, 60°

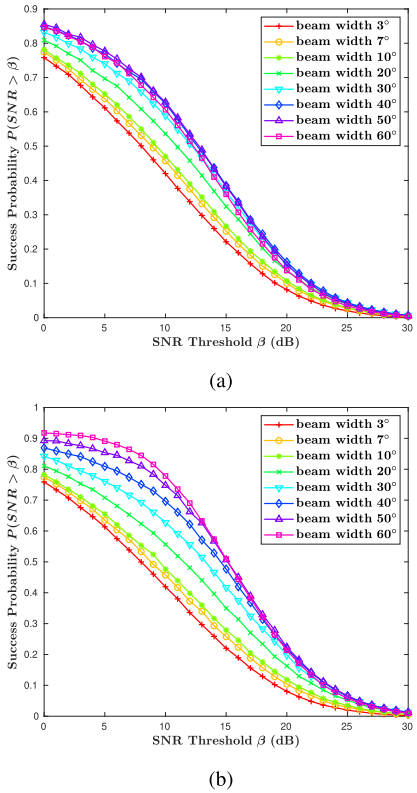


FIGURE 9. Success probability versus SNR threshold β for different antenna beamwidth for (a) 3GPP antenna model and (b) ideal sector antenna model.

under 3GPP and ideal sector antenna pattern respectively. With ideal sector antenna pattern, success probability of Eve increases with increasing beamwidth of Alice. With 60° beamwidth Eve has very high probability of eavesdropping even with higher SNR threshold requirements. The eavesdropping probability reduces drastically when Alice uses antenna pattern with narrow beamwidths of 3°, 7° and 10°. Success probability for different beamwidths under 3GPP antenna model also shows similar trend as that of ideal sector antenna model. But the success probability for 3GPP antenna model is lower than that of ideal sector pattern as the mainlobe gain of 3GPP antenna pattern varies with the beam direction. Even if Eve is in LOS sector of Alice, Eve will see a lower antenna gain if the boresight angle of Eve is not perfectly aligned with Alice.

2) EFFECT OF EVE'S ANTENNA

The success probability of Eve to eavesdrop Alice's communication varies depending on the antenna used by Eve. If Eve could use a narrow beam width high gain antenna, she could eavesdrop on Alice's communication even from longer distance. Eve could also benefit from weak reflections from ambient reflectors. We experimentally studied the impact of Eve's antenna beam width and gain on the eavesdropping success probability. We conducted experiments in the laboratory environment shown in Fig. 6c. We fixed Alice and Bob position at position labeled as *Tx* and *Rx3* in Fig. 6c.

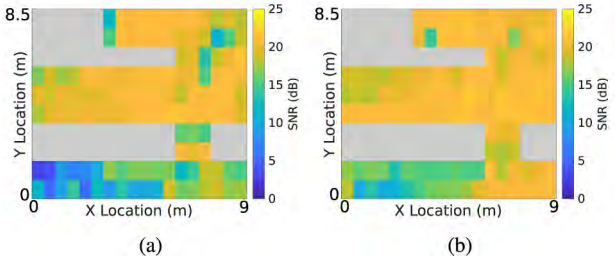


FIGURE 10. SNR of eavesdropped signal from alice. Eve uses an antenna with (a) 24 dBi gain and 11° beam width and (b) 34 dBi gain and 2.5° beam width.

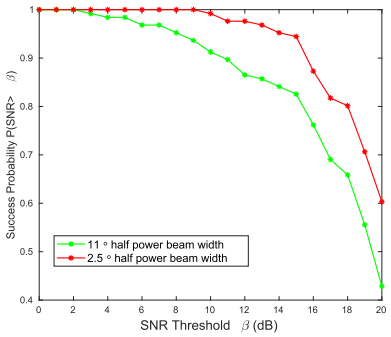


FIGURE 11. Success probability versus SNR threshold for different antenna gain and beam width of eve.

Throughout the experiment Alice to Bob communication sector is fixed at 20. The beam pattern of sector 20 is shown in Fig.7a. We used Vubiq 60 GHz receiver as Eve. For Eve, we used two directional horn antenna from Pasternack. One with 11° half power beam width and 24 dBi gain and another with 2.5° half power beam width and 34 dBi gain. The experiment area is divided into grids and in each grid position we focus on the strongest signal direction from Alice and record the SNR. The strongest signal direction could be towards Alice or towards favorable reflectors present in the experiment area. Fig. 10a and Fig. 10b shows the SNR of Alice signal eavesdropped by Eve with 24 dBi and 34 dBi gain antenna, respectively. With a higher gain antenna, Eve is able to eavesdrop on Alice signal with higher SNR than with lower gain antenna. Interestingly at locations behind Alice where Eve has LOS to Alice's back lobes, the SNR of overheard communication from Alice is significantly higher with 34 dBi antenna. This is due to a stronger signal from the reflector further amplified by Eve's high gain antenna. Fig.11 shows the success probability for different SNR thresholds. With 34 dBi antenna, the SNR of eavesdropped signal is higher than 15 dB over 90% of the eavesdropped area. On the other hand, with a 24 dBi antenna, the SNR is higher than 15 dB over only 80% of the eavesdropped area.

3) EFFECT OF AMBIENT REFLECTORS

In this section, we specifically discuss the effect of reflectors and Eve's antenna beam width and gain on her eavesdropping capabilities. We used a large cardboard of size $0.9m \times 0.9m$, a large metal plate of size $0.5m \times 1.2m$ (width $\times$ height) and a 21-inch computer screen as reflectors. We performed

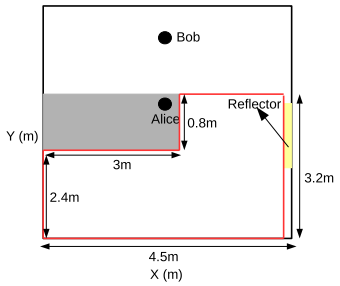


FIGURE 12. Floor plan of the indoor scenario for reflection experiments.

experiments for 2 types of Eve's antenna: (a) 11° beam width and 24 dBi gain and (b) 2.5° beam width and 34 dBi gain. The experiment area floor plan is shown in Fig. 12. Alice and Bob are placed at the location shown in the floor plan at a height of 1m. The space behind Alice from $(x = 0m, y = 2.4m)$ to $(x = 3m, y = 2.4m)$ is blocked so Eve can only point her beam towards the reflector. Alice communicates to Bob using antenna beampattern 20 shown in Fig. 7a. We placed the reflectors such that the side lobe between angle 120° and 150° of Alice's beampattern 20 points towards the reflector. Fig. 13 shows the received SNR at Eve for overhearing Alice's transmission to Bob for different reflector types and different antenna beam widths used by Eve. Our experiments showed that, owing to the irregular beampatterns of commercial mmWave devices, reflectors such as large cardboards, metal plates and computer screens of size comparable to the beam width of Alice's side lobe reflects significant beam. In particular, large cardboards and metal plates have many reflection points that could potentially act as sources of reflected signals for Eve. For an SNR threshold of 10 dB, 85% and 65% of eavesdropping area exceeds the SNR threshold at Eve with 2.5° antenna, 34 dBi gain and 11° antenna, 24 dBi gain, respectively for the cardboard reflector. For the metal reflector, the eavesdropping area reduces to 50% and 35% for 2.5° antenna, 34 dBi gain and 11° antenna, 24 dBi gain, respectively. Using narrow beam high gain antenna significantly helps Eve to eavesdrop on Alice's signal. On the other hand, smaller reflecting surfaces like computer screens reflects beam towards a particular spatial direction. If Eve is not exactly in the direction of the reflected signal, her eavesdropped signal SNR significantly decreases. For the same reason, using narrow beam to eavesdrop is not a wise choice for Eve. A wider beam antenna will help Eve to collect as much reflected energy as possible even if Eve is not exactly in the direction of reflection. The eavesdropping area for computer screen is 20% and 30% for 2.5° antenna, 34 dBi gain and 11° antenna, 24 dBi gain, respectively. Under opportunistic stationary attack, even if Eve could not point her antenna beam towards Alice she could still take advantage of the ambient reflectors in the environment, and point her antenna beam towards the reflectors.

4) EFFECT OF DENSITY OF REFLECTORS

As the density of reflectors in the environment increases, the probability of Eve finding an ambient reflector that could

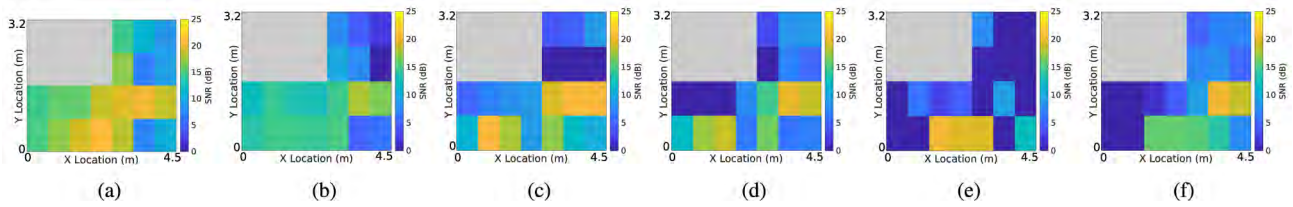


FIGURE 13. SNR at eve for different reflectors and different beam widths of eve's antenna; (a) cardboard and 2.5° beam width, (b) cardboard and 11° beam width, (c) metal plate and 2.5° beam width, (d) metal plate and 11° beam width, (e) computer screen and 2.5° beam width and (f) computer screen and 11° beam width.

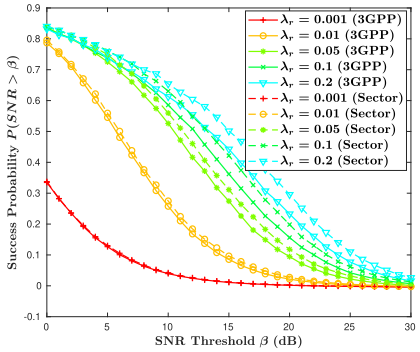


FIGURE 14. Success probability versus SNR threshold β for different reflector density for 3GPP antenna model and ideal sector antenna model.

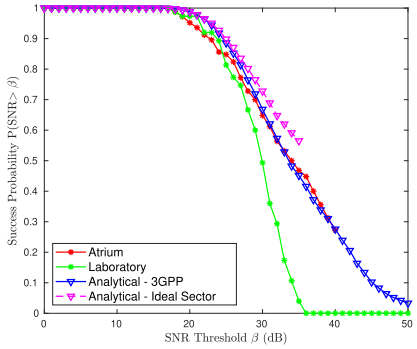


FIGURE 15. Active nomadic attack success probability versus SNR threshold β for simulation and experiments in the atrium and in the laboratory.

potentially serve as a reflected path to overhear Alice's transmission increases dramatically. Fig. 14 shows Eve's success probability for different reflector densities $\lambda_r = 0.001, 0.01, 0.05, 0.1, 0.2$. We can see that for $\lambda_r = 0.001$, the success probability is 0.33 for an SNR threshold of 0 dB. As the reflector density increases to $\lambda_r = 0.1$, Eve's success probability increases to 0.85. Also, it should be noted due to Eve's antenna misalignment, the success probability with 3GPP antenna is lower than that of success probability with sector antenna.

D. ACTIVE NOMADIC ATTACK

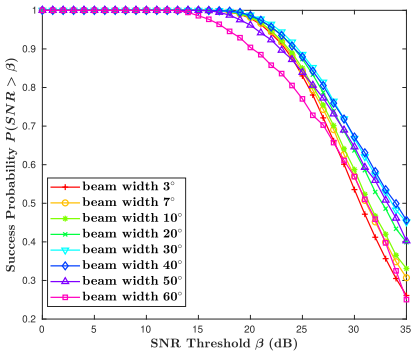
In this section, we present the analytical model evaluation and experimental results for our proposed active nomadic attack model described in Section IV. The analytical model in Section IV is evaluated with the parameters and set up described in Section V. The experiments were carried out in indoor laboratory and atrium environment described in Section V. We randomly deploy Alice and Bob in the environment. Alice and Bob communicates through the best sector found through the sector sweep mechanism. Eve is equipped with a 60 GHz 802.11ad compatible laptop to execute the protocol described in Section IV to estimate the sector between Alice and Bob and move to the sector.

1) EVE'S SUCCESS PROBABILITY UNDER ACTIVE NOMADIC ATTACK

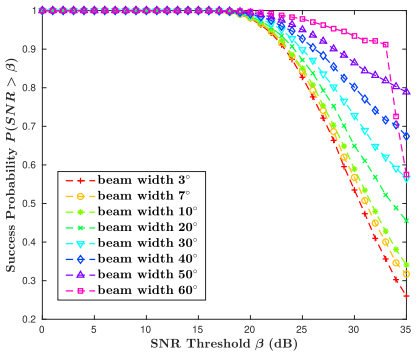
As described in the previous section, since Eve estimates the LOS region between Alice and Bob and moves to the region for eavesdropping, Eve has a higher probability of overhearing Alice's transmission than under opportunistic stationary attack. Fig. 15 shows Eve's success probability for different SNR thresholds. The success probability is shown for both the analytical model as well as for the experiments in the laboratory and in the atrium. We see that success probability using ideal sector antenna is higher than using 3GPP antenna pattern. In the active nomadic attack, it is very unlikely Eve's antenna will be in the boresight of the beampattern used by Alice since errors in estimating the location of Alice and subsequent LOS region estimation of Alice to Bob communication will translate to beam direction misalignment between Alice and Eve. Such antenna beam direction misalignment will significantly reduce the antenna gain seen by Eve. However, with ideal sector antenna, Eve's received power will not be affected as long as Eve's antenna beam direction is within the mainlobe beam of Alice. Fig. 15 also shows Eve's experimental success probability in the laboratory and in the atrium. The atrium where the experiments are performed is a large open space environment as shown in the floor plan Fig. 6d. Therefore, Eve has a better chance of moving to the LOS region between Alice and Bob. The atrium has glass walls on two sides. Eve has clear unobstructed LOS to Alice. In addition to that, the reflections from the glass side walls enhance the received power at Eve. This results in the success probability in the atrium significantly higher than the laboratory.

2) EFFECT OF ALICE BEAM WIDTH

Fig. 16 compares the eavesdropping probability for different beamwidth of Alice's antenna. For Eve to perform LOS attack, the LOS sector between Alice and Bob must be estimated. For wider beam antenna patterns, Eve has a high



(a)



(b)

FIGURE 16. Active nomadic attack success probability versus SNR threshold β for different antenna beamwidth for (a) 3GPP antenna model and (b) ideal sector antenna model.

accuracy of estimating Alice's sector and moving to the estimated region which results in higher probability for Eve to overhear Alice's transmission. Any antenna beam misalignment will not drastically reduce the received power at Eve. On the other hand, for narrow beam antenna, localization error might lead Eve to a neighboring sector than the actual LOS sector used by Alice. Also, beam misalignment with narrow beam antenna will drastically reduce the received signal power at Eve. Fig. 16a clearly demonstrates that wider beam patterns provides significant advantage to Eve to eavesdrop on Alice's transmission. Commercial 802.11ad routers and devices currently available in the market uses wider beam antenna patterns (some uses irregular beampatterns as wide as 30° to 60°). Even though mmWave communications offers significant resilient to passive eavesdropping due to directional antenna patterns, the analytical model validation and experiments show that the wider mainlobe beam patterns used by commercial devices poses significant eavesdropping threat.

3) EFFECT OF EVE'S ANTENNA DIRECTION ERROR ON SUCCESS PROBABILITY

In this section, we specifically study the beam direction error on Eve's probability to overhear Alice transmission. For this simulation, the beamwidth is fixed at 30° and the beam direction error is varied from 0° (perfect alignment) to $\frac{\theta_1}{2}$. Fig. 17 shows the eavesdropping success probability

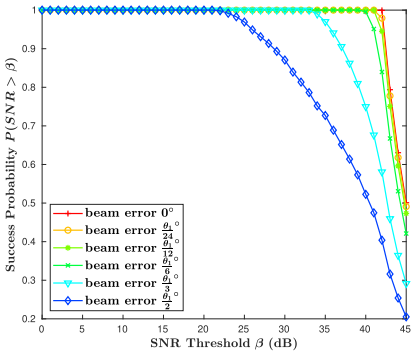


FIGURE 17. Active nomadic attack success probability versus SNR threshold β for different antenna direction error.

of Eve for different beam direction error. As long as the alignment error is within few degrees of the boresight of mainlobe of Alice, Eve's success probability is not significantly affected. Eve's ability to eavesdrop on Alice transmission drastically reduces when the alignment error moves Eve's beam direction away from the Alice antenna boresight significantly.

VI. CONCLUSION

It is often assumed in mmWave communication systems, it is practically infeasible for an eavesdropper to overhear the transmission from outside the direction of the main beam, due to the quasi-optical propagation characteristics. However, the presence of reflectors in the environment can significantly aid in eavesdropping through the reflected signal. Moreover, active nomadic attack based on the knowledge of 802.11ad protocol can further increase the successful eavesdropping possibility. In this work, we presented eavesdropping attack strategy for 802.11ad mmWave WLAN systems and evaluated the probability of successful overhearing of the transmission from Alice. From our analytical, and experimental studies, we show that the success probability of eavesdropping can be significant due to the presence of reflectors in the environment and the active eavesdropping attack.

APPENDIX A
3GPP ANTENNA GAIN DISTRIBUTION

From (2) when $\theta = \theta_\epsilon$, antenna gain is given by $G(\theta_\epsilon) = G_m \cdot 10^{-\frac{3}{10}(\frac{2\theta_\epsilon}{\theta_{3dB}})^2}$. Since the antenna gain $G(\theta_\epsilon)$ is a function of beam alignment error θ_ϵ which is modeled as a random variable with truncated normal distribution given by (3), by using method of transformation of random variables, the PDF of antenna gain $G(\theta_\epsilon)$ is given by

$$f_{G(\theta_\epsilon)}(x) = f_{\theta_\epsilon}\left(\frac{\theta_{3dB}}{2}\sqrt{\left(\frac{10}{3}log10\left(\frac{G_m}{x}\right)\right)}\right) \times \left|\frac{\mathrm{d}\left(\frac{\theta_{3dB}}{2}\sqrt{\left(\frac{10}{3}log10\left(\frac{G_m}{x}\right)\right)}\right)}{\mathrm{d}x}\right|, \quad (23)$$

which can be easily shown as

$$\frac{\theta_{3dB} f_{\theta_\epsilon}\left(\theta_{3dB}\sqrt{\left(\frac{5}{6}log10\left(\frac{G_m}{x}\right)\right)}\right)}{ln(10)x\sqrt{\frac{6}{5}log10(\frac{G_m}{x})}}.$$

APPENDIX B
REFLECTION PROBABILITY

A reflected path exists between Alice and Eve when the centers of the obstacles does not fall within the blockage area *ABEHLKJZD* in Fig. 4. Therefore the reflected probability P_{Ref} is given by

$$P_{Ref} = P(N = 0) = e^{-\mathbb{E}(N)} \tag{24}$$

Substituting (13) in (24) we get the expression given in (14).

APPENDIX C
DISTANCE ESTIMATION DISTRIBUTION

The estimated distance $d_{est} = \sqrt{\frac{P_{tx}G_{tx}(\theta)}{(\frac{4\pi}{\lambda})^2 P_{rx}}}\sqrt{G_{rx}(\theta_\epsilon)}$ is a function of the antenna gain $G_{rx}(\theta_\epsilon)$ which is a random variable with distribution given by (4) for 3GPP antenna model and (5) for ideal sector antenna model. The CDF of d_{est} is given by

$$\begin{aligned} F_{d_{est}}(x) &= P(d_{est} \leq x) \\ &= P\left(\sqrt{\frac{P_{tx}G_{tx}(\theta)}{(\frac{4\pi}{\lambda})^2 P_{rx}}}\sqrt{(G_{rx}(\theta_\epsilon))} \leq x\right) \\ &= P\left(G_{rx}(\theta_\epsilon) \leq x^2 \frac{\left(\frac{4\pi}{\lambda}\right)^2 P_{rx}}{P_{tx}G_{tx}(\theta)}\right) \\ &= F_{G_{rx}(\theta_\epsilon)}\left(x^2 \frac{\left(\frac{4\pi}{\lambda}\right)^2 P_{rx}}{P_{tx}G_{tx}(\theta)}\right) \end{aligned} \tag{25}$$

REFERENCES

[1] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[2] E. Perahia, C. Cordeiro, M. Park, and L. L. Yang, "IEEE 802.11ad: Defining the next generation multi-Gbps Wi-Fi," in *Proc. 7th IEEE Consum. Commun. Netw. Conf. (CCNC)*. Jan. 2010, pp. 1–5.

[3] F. Fuschini, S. Hafner, M. Zoli, R. Müller, E. Vitucci, D. Dupleich, M. Barbiroli, J. Luo, E. Schulz, V. Degli-Esposti, and R. S. Thomä, "Analysis of in-room mm-wave propagation: Directional channel measurements and ray tracing simulations," *J. Infr., Millim., THz. Waves*, vol. 38, no. 6, pp. 727–744, 2017.

[4] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band*, IEEE Standard 802.11ad-2012, 2012.

[5] D. Steinmetzer, M. Schulz, and M. Hollick, "Lockpicking physical layer key exchange: Weak adversary models invite the thief," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2015, p. 1.

[6] C. Rusu, N. González-Prelcic, and R. W. Heath, Jr., "An attack on antenna subset modulation for millimeter wave communication," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 2914–2918.

[7] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 335–343.

[8] Y. Zhu, Y. Ju, B. Wang, J. Cryan, B. Y. Zhao, and H. Zheng, "Wireless side-lobe eavesdropping attacks," 2018, *arXiv:1810.10157*. [Online]. Available: https://arxiv.org/abs/1810.10157

[9] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," Tech. Rep., 2019.

[10] T. Bai and R. W. Heath, Jr., "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2014.

[11] M. Cheng, J.-B. Wang, Y. Wu, X.-G. Xia, K.-K. Wong, and M. Lin, "Coverage analysis for millimeter wave cellular networks with imperfect beam alignment," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8302–8314, Sep. 2018.

[12] G. Yang, J. Du, and M. Xiao, "Analysis on 60 GHz wireless communications with beamwidth-dependent misalignment," 2016, *arXiv:1611.07867*. [Online]. Available: https://arxiv.org/abs/1611.07867

[13] J. Wildman, P. H. J. Nardelli, M. Latva-Aho, and S. Weber, "On the joint impact of beamwidth and orientation error on throughput in directional wireless Poisson networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 7072–7085, Dec. 2014.

[14] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[15] *TP-Link Talon AD7200 Multi-Band Wi-Fi Router*. Accessed: May 30, 2018. [Online]. Available: http://www.tp-link.com/us/products/details/cat-5506_AD7200.html

[16] *60 GHz Development System*. Accessed: Jun. 3, 2018. [Online]. Available: https://www.pasternack.com/60-ghz-development-system-low-phase-noise-pem009-kit-p.aspx

[17] S. Nie, M. K. Samimi, T. Wu, S. Deng, G. R. MacCartney, Jr, and T. S. Rappaport, "73 GHz millimeter-wave indoor and foliage propagation channel measurements and results," NYU WIRELESS, New York, NY, USA, Tech. Rep. TR-2014–003, 2014.

[18] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, Jun. 2011.

[19] S. Geng, J. Kivinen, X. Zhao, and P. Vainikainen, "Millimeter-wave propagation channel characterization for short-range wireless communications," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 3–13, Jan. 2009.

[20] A. Thornburg, T. Bai, and R. W. Heath, Jr., "Performance analysis of outdoor mmWave ad hoc networks," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4065–4079, Aug. 2016.

[21] I. Toyoda, *Reference Antenna Model With Side Lobe for TG3C Evaluation*, IEEE Standard 802.15-06-0474-00-003c, 2006.

[22] A. Thornburg and R. W. Heath, Jr., "Ergodic capacity in mmwave ad hoc network with imperfect beam alignment," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2015, pp. 1479–1484.

[23] *Channel Models for 60 GHz Wlan Systems*. Accessed: Jun. 3, 2018. [Online]. Available: http://www.ieee802.org/11/Reports/tgad_update.htm

[24] H. Xu, V. Kukshya, and T. S. Rappaport, "Spatial and temporal characteristics of 60-GHz indoor channels," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 3, pp. 620–630, Apr. 2002.

[25] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: Opportunities and challenges," *Wireless Netw.*, vol. 21, no. 8, pp. 2657–2676, 2015.

[26] T. Bai, R. Vaze, and R. W. Heath, Jr., "Analysis of blockage effects on urban cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5070–5083, Sep. 2014.

[27] N. A. Muhammad, P. Wang, Y. Li, and B. Vucetic, "Analytical model for outdoor millimeter wave channels using geometry-based stochastic approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 912–926, Feb. 2017.

[28] *Acer TravelMate P446-M*. Accessed: May 30, 2018. [Online]. Available: https://www.acer.com/ac/en/US/ content/professional-series/travelmatep4

[29] B. Langen, G. Lober, and W. Herzig, "Reflection and transmission behaviour of building materials at 60 GHz," in *Proc. 5th IEEE Int. Symp. Pers., Indoor Mobile Radio Commun., Wireless Netw.-Catching Mobile Future*, vol. 2, Sep. 1994, pp. 505–509.

[30] *Ad7200 Multi-Band Wi-Fi-Router*. Accessed: Mar. 25, 2019. [Online]. Available: https://static.tp-link.com/2018/201809/20180912/AD7200_2.0_Datasheet.pdf

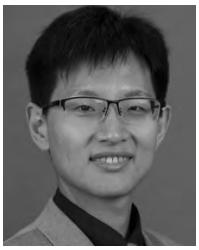
[31] D. Steinmetzer, D. Wegemer, M. Schulz, J. Widmer, and M. Hollick, "Compressive millimeter-wave sector selection in off-the-shelf IEEE 802.11ad devices," in *Proc. 13th Int. Conf. Emerg. Netw. Exp. Technol.*, 2017, pp. 414–425.
[32] *Wr-15 Waveguide Standard Gain Horn Antenna*. Accessed: Jun. 3, 2018. [Online]. Available: https://www.pasternack.com/single-antenna-operates-from-50-75-ghz-with-a-nominal-dbi-gain-wr-15-input-connectors-pe9881-24-p.aspx

SARANKUMAR BALAKRISHNAN (S'13) received the B.E. degree in electronics & communication engineering from Pondicherry University, India, in 2010, and the M.S. degree in electrical engineering from the National University of Singapore, Singapore, in 2013. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, University at Buffalo, The State University of New York. He was an Associate Scientist with Temesek Laboratories, Singapore, focusing on digital beamforming and wireless system design using Software Defined Radios. He also held an internship with the Wireless Technology Group, SONY US Research Center, focusing on mmWave wireless networks. His current research interest includes physical layer security for mmWave wireless networks.

PU WANG received the B.Eng. degree in electrical engineering from the Beijing Institute of Technology, China, in 2003, the M.Eng. degree in electrical and computer engineering from the Memorial University of Newfoundland, Canada, in 2008, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2013, under the supervision of Prof. I. F. Akyildiz. He was an Assistant Professor with the Department of Electrical Engineering and Computer Science, Wichita State University, from 2013 to 2017. He is currently an Assistant Professor with the Department of Computer Science, University of North Carolina at Charlotte. His current research interests include modeling, analysis, and stochastic optimization of networked systems, with applications in software defined networking, cyber-physical systems, the Internet of Things, wireless sensor networks, cognitive radio networks, and electromagnetic nanonetworks.

ARUPJYOTI (ARUP) BHUYAN received the M.Phil. and M.S. degrees and the Ph.D. degree in electrical engineering from Yale University, in 1985, 1986, and 1989, respectively.

He joined AT&T Bell Laboratories, in 1989, and became a part of Lucent Technologies and then Alcatel-Lucent. When he left to join the INL, he was the E2E Program Management Director in the 4G LTE Wireless Program for Advanced Services, such as the VoLTE (Voice over LTE) and eMBMS (evolved Multimedia Broadcast Multicast Services). He has extensive industry experience in wireless and telecommunications. He joined the Idaho National Laboratory (INL), in 2015, where his work focusses on the security aspects of wireless systems. He is currently a Wireless Researcher with INL's National & Homeland Security Directorate. His research interests include cyber secure physical layer for mmWave systems, secure and reliable cellular drone operation, and secure use of wireless in a nuclear plant.



ZHI SUN received the B.S. degree in telecommunication engineering from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2004, the M.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2011, where he was a Postdoctoral Fellow, from 2011 to 2012. He joined the Department of Electrical Engineering, University at Buffalo, The State University of New York, Buffalo, NY, USA, as an Assistant Professor, in 2012, where he is currently an Associate Professor. His research interests include reconfigurable mmWave communications, wireless communication and networking in extreme environments, metamaterial enhanced communication and security, physical-layer security, wireless intra-body networks, wireless underground networks, wireless underwater networks, and cyber physical systems. He was a recipient of the Outstanding Graduate Award at Tsinghua University, in 2007, the BWN Researcher of the Year Award at the Georgia Institute of Technology, in 2009, the Best Paper Award in IEEE GLOBECOM, in 2010, the Best Demo Award in IEEE INFOCOM, 2017, NSF CAREER Award, in 2017, UB Exceptional Scholar—Young Investigator Award, in 2017, and the Distinguished TPC Member Award in IEEE INFOCOM, 2018. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and Elsevier *Computer Networks* Journal.